UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/655,680	09/04/2003	Maclen Marvit	53635-0517	6508

29989 7590 08/07/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/655,680	MARVIT ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☒ Claim(s) *15,17,19-22, 37,39,41-44, 59,61,63-66* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20060731*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 28 June 2006.

2. Claims 1-66 are pending for examination.

3. Claims 1-66 are rejected.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned

with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-66 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-98 of U.S. Patent No. 6,625,734. Although the conflicting claims are not identical, they are not patentably distinct from each other because "managing access" and "controlling and tracking access" as applied to multimode (i.e., network) message traffic, irrespective of the packet, channel, or message (per se) nature of the data; and, "managing access to the key" and "deleting the key" as applied to key policy criteria, is clearly not patentably distinct.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1,3-14,16,18,23,25-36,38,40,45,47-58,60,62 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsumoto, U.S. Patent 6,215,877 B1.

6. As per claim 1; "A method for managing access to messages in a network, the method comprising the computer-implemented steps of:

receiving, from a first node in the network,

a request for both

a message identifier that

uniquely identifies the message and

a key that may be used

to encode the message [figures 4-11 and associated descriptions, whereas the key management server used to supply encryption/decryption keys used to service a multi-channel secured network communications chat server system (i.e., figure 4 and accompanying description) and further, upon chat channel establishment, the actual chat data is just message data that is sent across the network in encrypted form, and control of which is dependent on the subsequent decryption as controlled by the security policy established by the key management server. As per the Brief Summary of the invention (i.e., col. 2, lines 60-68), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

generating, in response to receiving the request,

both

the message identifier and

the key;

providing

both

the message identifier and

the key to the first node

to allow the message to be

encoded with the key

to generate an encoded message;

receiving, from a second node in the network,

a request for the key [figures 4-11 and associated descriptions, whereas the second terminal (node) requests the session key for subsequent decryption (decoding) of the first terminal originated chat (message) data as part of the one to one (node) communications (i.e., col. 4, lines 25- 36), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

providing the key to the second node

to allow

the encoded message to be

decoded and

the message to be

retrieved using the key; and

managing access to the key based upon

key policy criteria [figures 4-11 and associated descriptions, whereas when the chat communications is to be ended (i.e., all chat participants have signed of, and no

selected chat server channel specific traffic is occurring), the chat channel key is replaced with a newly generated key (i.e., col. 10, lines 22- 34), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 23, this claim is a medium embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

And further as per claim 45, this claim is an apparatus (system) claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

7. Claim 3 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein managing access to the key based upon key policy criteria includes

only providing the key to authorized entities in accordance with

the key policy criteria.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the use of public key authentication to verify key/ID requests to the key management server (i.e., col.3, lines 21-51), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 25, this claim is a medium embodied software claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

And further as per claim 47, this claim is an apparatus (system) claim for the method claim 3 above, and is rejected for the same reason provided for the claim 3 rejection.

8. Claim 4 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein the steps are performed at

a third node in the network that is

different from the first and second node.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is a characteristic of commercial chat systems/networks that they are multi-server in configuration so as to divide up the inherent functions of key/authentication/authorization among processing elements such that a chat system would have the chat (thread) service provider (i.e., AOL instant messenger ISP) establish key policy criteria, such as expiration time of the key as a function of the chat duration, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 26, this claim is a medium embodied software claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

And further as per claim 48, this claim is an apparatus (system) claim for the method claim 4 above, and is rejected for the same reason provided for the claim 4 rejection.

9. Claim 5 ***additionally recites*** the limitations that; "A method as recited in Claim 4,

wherein the steps are performed by

a key server executing at the third node.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is a characteristic of commercial chat systems/networks that they are multi-server in configuration so as to divide up the inherent functions of key/authentication/authorization among processing elements such that a chat system would have the chat (thread) service provider (i.e., AOL instant messenger ISP) establish key policy criteria, such as expiration time of the key as a function of the chat duration, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 27, this claim is a medium embodied software claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection.

And further as per claim 49, this claim is an apparatus (system) claim for the method claim 5 above, and is rejected for the same reason provided for the claim 5 rejection.

10. Claim 6 ***additionally recites*** the limitations that; "A method as recited in Claim 1, further comprising

verifying whether the first node is

authorized to obtain the key.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the use of public key authentication to verify key/ID requests to the key management server (i.e., col.3, lines 21-

51), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 28, this claim is a medium embodied software claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection.

And further as per claim 50, this claim is an apparatus (system) claim for the method claim 6 above, and is rejected for the same reason provided for the claim 6 rejection.

11. Claim 7 ***additionally recites*** the limitations that; "A method as recited in Claim 1,
wherein the request from the second node for the key
specifies the message identifier, and
the method further comprises
verifying that the second node is
authorized to receive the key.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the use of public key authentication to verify key/ID requests to the key management server (i.e., col.3, lines 21-51), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 29, this claim is a medium embodied software claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection.

And further as per claim 51, this claim is an apparatus (system) claim for the method claim 7 above, and is rejected for the same reason provided for the claim 7 rejection.

12. Claim 8 ***additionally recites*** the limitations that; "A method as recited in Claim 1, further comprising

generating and storing data that indicates that

the key was provided to

the first node or

the second node.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the use of channel status monitoring in order to account for the chat channel going to an unused state in order to generate a new channel key (i.e., col. 10, lines 22- 54), and further, the state change information pertaining to a channel going null constitutes information pertaining to a new key to be used in a subsequent chat communications, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 30, this claim is a medium embodied software claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection.

And further as per claim 52, this claim is an apparatus (system) claim for the method claim 8 above, and is rejected for the same reason provided for the claim 8 rejection.

13. Claim 9 ***additionally recites*** the limitations that; "A method as recited in Claim 1, further comprising

generating and storing data that indicates that

the encoded message was decoded at

the second node using the key.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is an inherent characteristic of commercial chat systems to store/log events for the purpose of billing chat participants for the chat service (i.e., AOL instant messenger if chat participants are paid subscribers of AOL ISP), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 31, this claim is a medium embodied software claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

And further as per claim 53, this claim is an apparatus (system) claim for the method claim 9 above, and is rejected for the same reason provided for the claim 9 rejection.

14. Claim 10 ***additionally recites*** the limitations that; "A method as recited in Claim 6, further comprising

generating and storing data that indicates that

the retrieved message was stored.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is an inherent characteristic of commercial chat systems to store/log events for the purpose of billing chat participants for the chat service (i.e., AOL instant messenger if chat participants are paid subscribers of AOL ISP), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 32, this claim is a medium embodied software claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection.

And further as per claim 54, this claim is an apparatus (system) claim for the method claim 10 above, and is rejected for the same reason provided for the claim 10 rejection.

15. Claim 11 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein the key policy criteria are managed at

a third node in the network that is

different than the first and second nodes.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is a characteristic of commercial chat systems/networks that they are multi-server in configuration so as to divide up the inherent functions of key/authentication/authorization among processing elements such that a chat system would have the chat (thread) service provider (i.e., AOL instant messenger ISP) establish key policy criteria, such as expiration time of the key as a function of

the chat duration, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 33, this claim is a medium embodied software claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection.

And further as per claim 55, this claim is an apparatus (system) claim for the method claim 11 above, and is rejected for the same reason provided for the claim 11 rejection.

16. Claim 12 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein the key policy criteria include one or more of

expiration date criteria,

subject matter criteria and

node identification criteria.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the chat system/network allows expiration of the public key (i.e., col. 17, claim 9), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 34, this claim is a medium embodied software claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection.

And further as per claim 56, this claim is an apparatus (system) claim for the method claim 12 above, and is rejected for the same reason provided for the claim 12 rejection.

17. Claim 13 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein the key policy criteria are

dynamically changed over time.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the chat system/network allows expiration of the public key (i.e., col. 17, claim 9), which as a minimum constitutes a 'dynamically changed ... key policy', clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 35, this claim is a medium embodied software claim for the method claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection.

And further as per claim 57, this claim is an apparatus (system) claim for the method claim 13 above, and is rejected for the same reason provided for the claim 13 rejection.

18. Claim 14 ***additionally recites*** the limitations that; "A method as recited in Claim 1, further comprising

generating meta data that specifies

an attribute of the message, and

wherein the step of deleting the key based upon key policy criteria includes

deleting the key by applying

the key policy criteria to the meta data.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas it is an inherent characteristic of commercial chat systems to store/log events for the purpose of billing chat participants for the chat service (i.e., AOL instant messenger if chat participants are paid subscribers of AOL ISP) such that it would have associated with the logged events, message associated data (meta) that would be handled (i.e., logged or deleted) by the same such key deletion policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 36, this claim is a medium embodied software claim for the method claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection.

And further as per claim 58, this claim is an apparatus (system) claim for the method claim 14 above, and is rejected for the same reason provided for the claim 14 rejection.

19. Claim 16 ***additionally recites*** the limitations that; "16. A method as recited in Claim 1, further comprising

providing location data to the second node that

uniquely identifies a location where the key is maintained.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the chat server and key management server are part of the same network, and mutually addressable by network

address (i.e., IP address, or chat channel address, figure 4 and accompanying description), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 38, this claim is a medium embodied software claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection.

And further as per claim 60, this claim is an apparatus (system) claim for the method claim 16 above, and is rejected for the same reason provided for the claim 16 rejection.

20. Claim 18 ***additionally recites*** the limitations that; "A method as recited in Claim 1, further comprising:

generating a digital signature of the message and

storing the digital signature in association with the message, and

providing the digital signature to

the second node to enable the second node to

validate the message.".

The teachings of Matsumoto (figures 4-11 and associated descriptions, whereas the using of a hash of the chat channel information (chat session, or chat message data), including information unique to the channel (col. 10, lines 6- 21), the hash clearly being used as a digital signature in association with the message, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 40, this claim is a medium embodied software claim for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection.

And further as per claim 62, this claim is an apparatus (system) claim for the method claim 18 above, and is rejected for the same reason provided for the claim 18 rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 2,24,46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto, U.S. Patent 6,215,877 B1, and further in view of Boneh, D. et al, "A revocable backup system", USENIX security Conference, pp. 91-96, 1996.

22. Claim 2 ***additionally recites*** the limitations that; "A method as recited in Claim 1, wherein managing access to the key based upon key policy criteria includes

deleting the key based upon

the key policy criteria.".

Matsumoto fails to teach of deleting the key as a function of specified key policy.

Boneh et al teaches of using the deletion of a generally centrally accessible encryption key to prevent access to file data and equivalent backup without having to access all copies of the backed up (tapes) so as to effectively deny access to the data (Abstract). A key file consisting of the secured keys and various key management policy attributes is stored and manipulated via various user interface routines (section 2, 3). Thus, key deletion is responsive to key file key policy.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to be motivated to combine the Matsumoto chat server communications key server invention with the Boneh et al encrypted file and associated backup file key deletion invention, in order to have the file that would reside on intermediate network nodes of a chat network to be effectively access controlled via the Boneh et al key deletion via specified key security policy.

Such motivation exists because the Matsumoto chat message data resides in network computer nodes as a file as it traverses the network, and thus requires effective deletion (i.e., permanent denied access via decoding key deletion), the same as if the file merely resides as a file on a computer or associated computer backup tape, as in the Boneh et al invention (Boneh, Abstract).

And further as per claim 24, this claim is a medium embodied software claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection.

And further as per claim 46, this claim is an apparatus (system) claim for the method claim 2 above, and is rejected for the same reason provided for the claim 2 rejection.

Allowable Subject Matter

23. Claims 15,17,19-22, 37,39,41-44, 59,61,63-66 are objected to as being dependent upon a rejected base claim, but would be allowable, subject to the above double patenting restrictions, if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

24. Applicant's arguments filed 28 June 2006 have been fully considered but they are not persuasive. As described above, the distinction between message level encryption and channel data so encrypted is not patently distinct.

Conclusion

25. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
PRIMARY EXAMINER

08/02/06

Ronald Baum

Patent Examiner